IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

ZAPFRAUD, INC., Plaintiff, v. FIREEYE, INC., Defendant.	)	Civil Action No. 19-1688-CFC
ZAPFRAUD, INC., Plaintiff, v. MIMECAST NORTH AMERICA, INC., MIMECAST UK LIMITED and MIMECAST SERVICES LTD., Defendants.	)	Civil Action No. 19-1690-CFC
ZAPFRAUD, INC., Plaintiff, v. PROOFPOINT, INC., Defendant.	)	Civil Action No. 19-1691-CFC

REPORT AND RECOMMENDATION

Pending before the Court in these three patent infringement cases are motions filed by Defendant FireEye, Inc. ("FireEye"), Defendants Mimecast North America, Inc., Mimecast UK Limited and Mimecast Services Ltd. ("Mimecast") and Defendant Proofpoint, Inc. ("Proofpoint," and collectively with FireEye and Mimecast, "Defendants"), pursuant to Federal Rule of Civil Procedure 12(b)(6) (the "Motions"). (Civil Action No. 19-1688-CFC, D.I. 31; Civil Action No.

19-1690-CFC, D.I. 31; Civil Action No. 19-1691, D.I. 31) With their Motions, Defendants argue that the patents asserted against them—United States Patent Nos. 10,277,628 (the "'628 patent") and 10,609,073 (the "'073 patent")—are directed to patent-ineligible subject matter pursuant to 35 U.S.C. § 101 ("Section 101"). For the reasons that follow, the Court recommends that the Motions be GRANTED.

I. BACKGROUND

A. Factual Background

The two patents-in-suit, both titled "Detecting Phishing Attempts," share a common specification.[1] The patents relate to systems and methods for detecting fraud or phishing attempts in e-mail communications using various disclosed techniques.

In providing context for the invention, the specification's "Background of the Invention" section first explains that individuals are "increasingly us[ing] electronic mail to communicate with one another for personal and business reasons." ('628 patent, col. 1:13-14) But it explains that these e-mail users also face a problem: that "unscrupulous individuals can use electronic mail for nefarious purposes, such as to send unwarranted advertising email (e.g., SPAM) and perpetrate fraud against victims." (*Id.*, col. 1:15-18) This fraud might include a scam like a "phishing scam, in which criminals contact unsuspecting Internet users using messages that appear to be authored by legitimate entities such as banks, with the goal of tricking the victims into clicking on links in the messages and providing banking credentials (e.g., usernames and passwords) or other sensitive information." (*Id.*, col. 3:45-50)

The specification then notes that certain prior art systems and methods had attempted to address this problem by identifying and filtering out these "nefarious" e-mails. More

[1] As such, the Court will cite below only to the '628 patent, unless otherwise noted.

specifically, the patents explain that one such technique "is the blacklisting of certain terms . . . where the presence of a blacklisted term in a message automatically results in the classification of the message as SPAM." (*Id*., col. 1:18-21; *see also* D.I. 29 at ¶¶ 27, 47) However, it notes a problem with this type of prior art approach that allows it to be "defeated by the unscrupulous individual": that the wrongdoer could "use terms that a human would recognize" and that are very similar to (but not exactly the same as) the blacklisted word, and thus that "might not appear on a blacklist." ('628 patent, col. 1:22-26) The specification also explains that "blacklisting of terms can be problematic in preventing fraud, where the goal of a fraudster is often to craft a message that looks as legitimate as possible (e.g., using only terms that commonly appear in legitimate communications)." (*Id.*, col. 1:27-30) In other words, sometimes the fraudulent actor will utilize legitimate-sounding terms like "bank" or "account" in a phishing message, and which would not be on any blacklist; indeed, in such a case, a "phishing message might appear to a recipient to contain, verbatim, the text of a legitimate message sent by a legitimate entity" (but yet, for example, the phishing message might also contain a link to a harmful resource). (*Id*., cols. 3:64-4:7; *see also* D.I. 29 at ¶¶ 28, 48) This bad actor might also make use of legitimate-looking text, logos, symbols or other phraseology in their phishing e-mails. ('628 patent, col. 3:55-63) The patents note that this "degree of possible customization of scam messages [made] it particularly difficult for existing e-mail filters to provide sufficient protection[.]" (*Id.* col. 4:7-10)

Other sources of record describe additional prior art e-mail filtering systems, in place at the time of the invention, which attempted to identify deceptive e-mail messages. (D.I. 34 at 5-6) One of those was a system that "blacklisted" not certain known, problematic words or terms, but instead certain e-mail addresses known to be associated with fraud. (D.I. 32, ex. A at 139)

However, this approach also had its problems, in that it obviously could not block an e-mail address that had not yet been "reported as, or determined to be, malicious[.]" (*Id*.) Another system used a "conventional whitelist approach[,]" which "may erase all emails [from addresses] that are not on a whitelist" (i.e., that are not on a list of previously-approved e-mail addresses). (*Id*.) The problem with that system is that it can be overprotective: it might block e-mails that the user actually wants to receive and that are not in fact fraudulent. (*Id*.)

Because there "exist[ed] an ongoing need to protect against the victimization of legitimate email users[,]" ('628 patent, col. 1:31-32), the patented inventions attempted to provide a new and better system—one that met the above-referenced need, but that did so without blocking too many desired e-mails. The patented systems and methods do not employ a "blacklist" or "whitelist" approach, as in the prior art. Instead, as will be discussed further below, they attempt to identify e-mails that "appear[] to have been transmitted by an authoritative entity" by, *inter alia*, "computing a similarity distance" between: (1) either the display name or header associated with the e-mail at issue (i.e., the e-mail that might purport to come from an "authoritative entity") and (2) the display name or header actually associated with that authoritative entity, which is stored in a separate database. (*Id.*, col. 35:43-57; *see also id*., col. 7:22-27; D.I. 29 at ¶¶ 29, 49) The claims also require that the system or method will go on to make a determination of whether this legitimate-looking e-mail is in fact fraudulent and, if it is, will take certain action with that e-mail. ('628 patent, col. 36:4-28)

Additional facts about the patents-in-suit will be set out below in Section III.

B. Procedural Background

Plaintiff filed its initial Complaint in all three actions on September 10, 2019. (*See, e.g.*, D.I. 1)[2] The currently operative complaint in all three actions is the Second Amended Complaint, in which Plaintiff alleges that Defendants directly, indirectly and willfully infringe at least claim 1 of the '628 patent and at least claim 1 of the '073 patent. (*See, e.g.*, D.I. 29)

All Defendants filed their respective Motions on May 22, 2020. (D.I. 31; Civil Action No. 19-1688-CFC, D.I. 31; Civil Action No. 19-1691-CFC, D.I. 31) FireEye and Proofpoint simply joined Mimecast's Motion and all of Mimecast's briefing in support thereof. (Civil Action No. 19-1688-CFC, D.I. 31; Civil Action No. 19-1691-CFC, D.I. 31) These three cases have been referred to the Court by United States District Judge Colm F. Connolly to hear and resolve the pending Motions. (*See* D.I. 33; Civil Action No. 19-1688-CFC, D.I. 32; Civil Action No. 19-1691-CFC, D.I. 32) The Motions were fully briefed as of June 19, 2020, (*see, e.g.*, D.I. 36), and the Court heard oral argument on the Motions on September 18, 2020, (D.I. 44, hereinafter, "Tr.").

II. STANDARD OF REVIEW

The instant Rule 12(b)(6) Motions assert that certain claims of the patents-in-suit are directed to patent-ineligible subject matter. The Court has often set out the relevant legal standards for review of such a motion, including in *Genedics, LLC v. Meta Co.*, Civil Action No. 17-1062-CJB, 2018 WL 3991474, at *2-5 (D. Del. Aug. 21, 2018). The Court hereby incorporates by reference its discussion in *Genedics* of these legal standards and will follow those standards herein. To the extent consideration of Defendants' Motions necessitates

[2] Unless otherwise noted, citations below are to the docket in the Mimecast action, Civil Action No. 19-1690-CFC, which is representative of all three actions for our purposes.

discussion of other, related legal principles, the Court will set out those principles in Section III below.

III. DISCUSSION

In assessing the eligibility of the challenged claims of the patents, the Court will first discuss which of these claims will be addressed herein as representative. Thereafter, it will analyze the relevant claims under the test for patent eligibility set out in *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208 (2014).

A. Representative Claim at Issue

For purposes of the Motions, Defendants have asserted that claim 14 of the '628 patent is representative as to their arguments that all of the asserted claims of both patents-in-suit are patent ineligible. (D.I. 32 at 6 ("Claim 14 of the '628 patent is representative."); *id.* at 7 ("The '073 patent's . . . claims are materially the same, but are even *broader* . . . .") (emphasis in original)) At oral argument, Plaintiff agreed that it was permissible for the Court to analyze claim 14 as to the bulk of Defendants' eligibility arguments. (Tr. at 94) But in its briefing and at oral argument, Plaintiff also asserted that even if claim 14 and other related asserted claims are deemed ineligible, claims 4 and 5 of the respective patents should nevertheless survive the Motions. (D.I. 34 at 20; Tr. at 94)[3] Therefore, below the Court will take up the *Alice* analysis as to claim 14 first. Thereafter, it will address the two other claims.

B. Claim 14

1. *Alice*'s Step One

[3] Because the text of claims 4 and 5 of the '628 patent are materially the same as that of claims 4 and 5 of the '073 patent, the Court will (as the parties did in their briefing and at oral argument) treat claims 4 and 5 of the '628 patent as representative of claims 4 and 5 of the '073 patent.

As we begin the step one analysis, the Court will first set out the content of claim 14:

> **14.** A method for detecting attempted deception in an electronic communication, comprising:
>
> receiving, by at least one server, an electronic communication addressed to a user of a client device;
>
> parsing, by the at least one server, a display name associated with the electronic communication;
>
> determining, by at least one classifier component executing on one or more processors, that the electronic communication appears to have been transmitted on behalf of an authoritative entity by:
>
> computing a similarity distance between the display name and at least a name of the authoritative entity, wherein the name of the authoritative entity is retrieved from the at least one of the profile and a content database, wherein the similarity distance is computed by comparison of items by at least one of:
>
> basing the comparison on at least one of a match between the display name associated with the electronic communication and the display name of the authoritative entity, and
>
> a match between headers associated with the electronic communication and headers associated with the authoritative entity,
>
> wherein the matches are determined by at least one of:
>
> determining that the compared items are the same, determining that the compared items have a Hamming distance below a threshold value, determining that the compared items have an edit distance below a threshold value, determining that a support vector machine indicates a similarity based on previously trained examples, determining a similarity score based on how many characters were replaced by characters of sufficient similarity and performing at least one normalization followed by a comparison;
>
> determine, by the at least one classifier component, that the electronic communication was not transmitted with authorization from the authoritative entity;
>
> based at least in part on determining that the electronic communication appears to have been transmitted on behalf of the

> authoritative entity and determining that the electronic communication was not transmitted with authorization from the authoritative entity, perform a security determination, by the at least one server, including classifying the electronic communication, wherein the classifying includes two or more security classifications including good and bad; and
>
> based at least in part on the security determination resulting in a bad classification, perform an action by the at least one server comprising at least one of erasing the electronic communication, marking up the electronic communication at least in part by adding a warning or an explanation, flagging the electronic communication, forwarding the electronic communication to a third party, placing the electronic communications in the spam folder, and forwarding the electronic communication to a repository.

('628 patent, cols. 35:33-36:27)

In *Alice*'s first step, the "'directed to' inquiry applies a stage-one filter to claims, considered in light of the specification, based on 'whether their *character as a whole*'" or their "focus" is directed to excluded subject matter. *Enfish LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016) (quoting *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015) (emphasis added)). Here, Defendants argue that the asserted claims of the patents-in-suit, including claim 14, are "directed to" the abstract idea of "identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly[.]" (D.I. 32 at 10) Plaintiff does not dispute that "identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly" is an abstract idea, and the Court agrees that it is. The concept seems to be one "devoid of a concrete or tangible application[,]" *Ultramercial, Inc. v. Hulu LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014), and the concept is "untethered from any real-world application[,]" *CLS Bank Int'l v. Alice Corp. Pty. Ltd.*, 717 F.3d 1269, 1286 (Fed. Cir. 2013) (Lourie, J., concurring).

But Plaintiff asserts that claim 14 and the other asserted claims are not, in fact, "directed to" this abstract idea. Rather, Plaintiff argues that Defendants oversimplify the patents, which solve unique problems for existing electronic communications technologies. (D.I. 34 at 3, 6-7, 11-14) In making this argument, Plaintiff asserts that the patents claim a three-step approach to electronic communication security by:

> (1) "[D]etermin[ing] whether an incoming communication would appear trustworthy" (i.e., in the language of the claim, whether the e-mail communication "appears to have been transmitted on behalf of an authoritative entity") by "computing a similarity distance" (i.e., determining whether there is a "match") between the display name or headers associated with the e-mail and the display name or headers associated with the entity that are located in, for example a separate content database;
>
> (2) "[A]ssess[ing] that communication to determine if it was indeed transmitted with authorization from the authoritative entity"; and
>
> (3) If the e-mail is not from an authoritative entity, despite initially appearing to be, "classify[ing] it as 'bad' and dispos[ing] of it[.]"

(*Id.* at 4, 6-7 (internal quotation marks and citation omitted); *see also* '628 patent, FIG. 3 (setting out these steps)) Plaintiff's argument is that the claims are directed to a "'more flexible and nuanced' email classification" than Defendants' articulated abstract idea. (D.I. 34 at 13 (citing *id*. at 4-7)) For the four reasons set out below, however, the Court disagrees.

First, the way that Plaintiff articulates the invention's three-step approach (i.e., what the Plaintiff is saying is the invention's focus) sounds *a lot like* the asserted abstract idea at issue ("identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly"). (D.I. 36 at 2 ("ZapFraud's own description of its 'multi-step approach' tracks [the abstract idea.]")) Plaintiff basically describes step one as being about identifying messages

that appear to be from a trustworthy source. Step two is said to be about identifying deceptive messages. And step three is said to be about taking action accordingly. (*See id.*; Defendants' Hearing Presentation, Slide 11)

Second, the patent specification[4] describes the invention at issue in broad terms that seem consistent with this abstract idea. The title of the patent is simply "Detecting Phishing Attempts[.]" ('628 patent, Title) The patent's "Abstract" describes the invention in far-reaching language—language that also pretty fairly tracks Defendants' articulation of the abstract idea:

> Classifying electronic communications is disclosed. An electronic communication is received. A first likelihood that a potential recipient of the electronic communication would conclude that the communication was transmitted on behalf of an authoritative entity is determined. An assessment of a second likelihood that the received communication was transmitted with authorization from the purported authoritative entity is performed. The electronic communication is classified based at least in part on the first and second lik[e]lihoods.

(*Id.*, Abstract) Moreover, when the patentee was articulating the "need" for the patented invention in the patent's "Background of the Invention" section, it did so in a very open-ended way: "[t]here therefore exists an ongoing need to protect against the victimization of legitimate email users." (*Id.*, col. 1:31-32)

[4] In order to determine what a patent claim is really "directed to" at step one, the Federal Circuit has encouraged district courts to consider the content of the patent's specification. *Cf. Enfish*, 822 F.3d at 1337 (indicating that it is appropriate to look to a patent's specification to determine whether a claim of the patent is "directed to" a particular concept, and that if a claim contains a particular element that is described by the patent's specification as what the "present invention comprises[,]" this suggests that the claim may be directed to that element or concept) (internal quotation marks and citation omitted); *Internet Patents Corp.*, 790 F.3d at 1348 (same and noting that if a concept is described in the patent as being "the innovation over the prior art" or the "essential, most important aspect" of the patented invention, that suggests that the claim is directed to that concept) (internal quotation marks and citation omitted).

Third, as Defendants argue, (D.I. 36 at 3), apart from "generic computer-implemented steps, there is nothing in the claim[itself] that foreclose[s it] from being performed by a human[.]" *Intellectual Ventures 1 LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016). As Defendants note (and as the patents seem to underscore), the problem that the claim is attempting to address is a "very human problem": one in which a nefarious person seeks to trick a potential victim by sending the victim a communication that appears to be from a trusted source, but in reality is not. (Tr. at 15; *see also* Defendants' Hearing Presentation, Slide 5; '628 patent, col. 4:12-13 ("Described herein are techniques for protecting vulnerable users from malicious entities . . . .")).[5] And in setting out how it attempts to address this problem via claim 14, the patent indicates that the claimed steps are not all that complicated to implement—thus underscoring why it is not hard to picture these steps being completed by a human. For example, in order to "comput[e] a similarity distance" between the display name[6] of the e-mail and the name of the authoritative entity (so as to determine whether the e-mail appears to have been transmitted by an authoritative entity), the method requires only a "determin[ation] that the compared items *are the same*[.]" ('628 patent, cols. 35:45-36:3 (emphasis added); *see also* Tr. at 51 (Defendants' counsel noting that "at this level, we're at a very human process that a human

[5] Strangely, in attempting to make the point that the patented invention is attempting to solve something that is not a "human problem" but instead a "computer problem," Plaintiff pointed the Court to an outside-the-record portion of Mimecast's website, wherein Mimecast describes the problem by stating that "too many security teams are looking solely for a technical solution to what is *largely a human problem*." (Plaintiff's Hearing Presentation, Slide 18 (emphasis added) (*cited in* Tr. at 85-86))

[6] According to Plaintiff, a "display name" in an e-mail is the name of the person or entity, visible in the e-mail, that corresponds to a particular e-mail address for the person or entity that purportedly sent the e-mail. (Tr. at 72)

can do accurately[:] look at the two names and see if they're the same"))[7] As for the claimed step of determining that the e-mail was not, in fact, sent by an authoritative entity, claim 14 does not require any particular way to do that, other than to use a "classifier component" and by noting that the e-mail must ultimately be classified (e.g., as "good" or "bad"). ('628 patent, col. 36:4-16) And as for the third step, the method simply requires that "an action" be taken once the e-mail is determined to be deceptive (i.e., a "bad" e-mail), which can include "adding a warning" or "flagging" the e-mail. (*Id.*, col. 36:18-28)

Thus, as Defendants suggest, although claim 14 invokes a computer to perform at least part of the method, a "human receiving an e-mail can—and would—perform all of the claimed method steps (putting aside generic computer processing): receive a message, look at the sender's name, determine that it appears to be (but is not) from a trusted source, and dispose of it." (D.I. 36 at 3; *see* Tr. at 38 ("[C]omputing a similarity distance, determining by comparing and matching certain things and determining that they're the same, those are all part of the

[7] Of course, claim 14 does allow that this step could be accomplished by other means, such as by "determining that the compared items have a Hamming distance below a threshold value, determining that the compared items have an edit distance below a threshold value, determining that a support vector machine indicates a similarity based on previously trained examples, [or] determining a similarity score based on how many characters were replaced by characters of sufficient similarity and performing at least one normalization followed by a comparison[.]" ('628 patent, cols. 35:60-36:3) As Plaintiff notes, those various alternate means do take up a lot of space in the claim, and some of them (i.e., the use of a "support vector machine") might be difficult to align with a human counterpart. (D.I. 34 at 18) But the Court agrees with Defendants, (Tr. at 38), that because the claim *could* be satisfied simply by determining that the compared items are "the same," it is appropriate to focus on that permutation (i.e., the broadest/least specific permutation of the claimed step) in evaluating the full breadth of the claim. (D.I. 32 at 17-18) After all, "optional elements do not narrow [a] claim because they can always be omitted." *In re Johnston*, 435 F.3d 1381, 1384 (Fed. Cir. 2006). And as the Supreme Court of the United States has explained, "the concern that drives [Section 101 is] one of pre-emption." *Alice Corp.*, 573 U.S. at 216. So it stands to reason that in assessing the claim, either at *Alice*'s step one or step two, one must consider the claim in its broadest, most-possibly-pre-emptive permutation.

abstract idea because that's what a human would do anyway."); *see also id*. at 18, 20; D.I. 34 at 21 (Plaintiff acknowledging that the claimed method attempts to mimic "how a human would perceive an e-mail")) In fact, as Defendants point out, (D.I. 36 at 4-5; Defendants' Hearing Presentation, Slide 12), the patent specification explains that the patentee contemplated using "*human* reviewers *instead of* or in addition to performing automated analysis . . . e.g., a member of the IT department reviewing an email" as one part of the claimed technique for determining that an e-mail is deceptive, and that the conclusion of the human review could "decide[] the disposition" of the deceptive e-mail. ('628 patent, col. 8:11-40 (emphasis added); *see also id*., col. 3:15-26 (noting that the techniques disclosed are meant to "incorporate[] what *end-users will interpret a message as being* with system information about the message") (emphasis added); *id*., col. 15:39-40; Tr. at 89-90) That makes it a lot more difficult to say (as Plaintiff does) that Defendants' human-analogue argument is far-fetched.

Moreover, as Defendants note, even outside of the e-mail or computer context, humans can take steps similar to those found in the claimed method in order to determine whether a message is authentic. This can happen when a person: (1) receives a letter purporting to be from an authoritative entity with which the person does business; (2) checks to make sure that the entity's name is spelled or is formatted in a way that the person knows from experience it should be; (3) if it is not, mentally classifies the message as one indicative of fraud; and (4) gets rid of the letter. (D.I. 32 at 2, 12; Tr. at 48-49) This all suggests that in claim 14, "computers are invoked merely as a tool" for implementing what is otherwise an abstract idea. *Enfish*, 822 F.3d at 1336. And that in turn helps to demonstrate that the claim is directed to a well-known, abstract idea or practice. *Symantec*, 838 F.3d at 1318 (noting that "with the exception of generic computer-implemented steps, there is nothing in the claims themselves that foreclose them from

being performed by a human, mentally or with pen and paper" and that this helped demonstrate that the claims were directed to an abstract idea at step one).

Plaintiff counters that "there is no support [for the idea that] humans can 'mental[ly]' practice the claimed steps to reliably identify fraudulent messages[,]" in light of the fact that the patentee "explained [in the patent and during prosecution] that users tend to trust and fall victim to impersonation scams . . . or mistake a legitimate mail for attempted fraud." (D.I. 34 at 16 (citing D.I. 32, ex. A at 183; '628 patent, cols. 3:41-4:11, 15:33-34)) Plaintiff is surely correct that the patentee did explain: (1) how sophisticated fraudsters can include various "legitimate"-sounding terms or phrases in a phishing e-mail, and that this sometimes fools a human user; and (2) that the claimed systems and methods could provide better "protection" from such scams than a user's own efforts or prior art solutions might. ('628 patent, cols. 3:41-4:11) Yet just because claim 14's method "automat[es]" a process that a human might perform, and thereby makes the performance of that process more accurate, this does not mean that there is not a ready human analogue to the claimed computerized process. Nor does it save the claim at *Alice*'s step one. *See Prod. Assoc. Techs. LLC v. Clique Media Grp.*, CV 17-05463-GW(PJWx), 2017 WL 5664986, at *6 (C.D. Cal. Oct. 12, 2017); *see also Planet Bingo, LLC v. VKGS, LLC*, 961 F. Supp. 2d 840, 851-52 (W.D. Mich. 2013) (finding at step one that "all of the method claims recit[ing] a computer-aided method for playing the game of Bingo . . . consist[] solely of mental steps which can be carried out by a human[,]" which helped to demonstrate that the claims were directed to the abstract idea of "managing/playing the game of Bingo[,]" and ultimately concluding that the claims were patent ineligible, despite the plaintiff's argument that the claims "improved efficiency and accuracy" in playing Bingo); (Tr. at 61-62 (Plaintiff's counsel acknowledging that caselaw from the United States Court of Appeals for the Federal Circuit

states that if a claimed invention simply "mak[es] more accurate" a human process via use of a computer, it would not be patent eligible)); *cf. OIP Techs., Inc. v. Amazon.com*, Inc., 788 F.3d 1359, 1363 (Fed. Cir. 2015) (concluding at step two that just because a computerized method might be able perform a task "more quickly or more accurately" than a human, this does not mean that the method is patent eligible). And again, the patent tells us that at least some portions of the claimed steps can be effectuated by "use of one or more human reviewers instead of or in addition to performing automated analysis." ('628 patent, col. 8:11-13) This just helps to emphasize that the patented inventions do what humans can do—and that the patent simply purports to do it more efficiently or more accurately than a human might.[8]

[8] Plaintiff makes a few other arguments about why claim 14 does not have a clear human analogue, but they too are wanting. For example, Plaintiff argues that Defendants' "human analogy fails to capture the unique problems presented by electronic communication" because the conventional prior art systems discussed in the patent/prosecution history and the problems they present regarding e-mail filtering "have no human equivalent." (D.I. 34 at 15) The Court is not necessarily sure that is so. As Defendants note, it does seem that the human mind can accomplish something similar to the use of a blacklist or whitelist. For example, a person could mentally determine that they will discard or not review any messages that purport to be from a certain type of sender (e.g., a marketer), or that they will certainly keep and review any messages that purport to be from another type of sender (e.g., a relative). (D.I. 36 at 4) But more importantly, the focus here is on whether the *claimed solution* has a human analogue that is easily recognizable, and it does.

Additionally, Plaintiff argues that Defendants' human analogy fails to account for certain claim limitations "unique to the computer environment" such as matching a "domain name" of an incoming e-mail or using a "support vector machine" as one option to determine similarity. (D.I. 34 at 15 (internal quotation marks and citations omitted)) But if a claim "'simply add[s] conventional computer components to well-known . . . practices,'" the claim is still directed to an abstract idea. *In re TLI Commc'ns LLC Patent Litig.*, 823 F.3d 607, 612 (Fed. Cir. 2016) (citation omitted); *see also Twilio, Inc. v. Telesign Corp.*, 249 F. Supp. 3d 1123, 1144-46 (N.D. Cal. 2017) (finding that even though the claim at issue was limited to "[electronic] message routing[,]" that claim was still directed to an abstract idea because it simply applied an abstract idea to a certain technological environment).

Fourth, simply because the patent states that it claims an improvement over prior art filtering systems, that is not sufficient to demonstrate that claim 14 is "directed to" something narrower than the purported abstract idea. To be sure, the specification does assert that the claimed inventions do something that the prior art systems did not do. The patents explain how the claimed systems/methods are better than existing e-mail filtering technology (like a blacklist) because:

> [T]echniques disclosed herein can be used to combine an assessment of the likely end-user interpretation of the message (including the apparent sender email address, friendly/display name and message content) with an assessment of whether the apparent sender matches the actual sender, and to take actions in response, such as filtering actions or reporting actions.

('628 patent, col. 3:15-22; *see also id*., col. 1:19-30 (*cited in* D.I. 34 at 6)) And during prosecution, the patentee made the case to the Examiner that the claims were an improvement over the prior art because (unlike prior art solutions like blacklists or whitelists) the claims "detect attempted deception in an electronic communication by identifying communications where the sender appears trustworthy in the communication, but is not" and that "[c]urrent approaches do not perform such a determination." (D.I. 32, ex. A at 139 (cited in D.I. 34 at 6))[9]

[9] In light of this disclosure, the Court also disagrees with another counter-argument that Plaintiff made during oral argument. There, Plaintiff's counsel argued that "if you actually take Mimecast's articulation of the abstract idea at its word[], it would envelope th[e] conventional solutions" that are referenced in the specification's discussion of the prior art. (Tr. at 61; *see also id*. at 64) In other words, Plaintiff was arguing that claim 14 could not be directed to "identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly" because the prior art e-mail filters that are disparaged in the patent would *also* be captured by that concept. Plaintiff's point was that it would not make sense to conclude that the claim is directed to a concept broad enough to cover systems that the patent was emphatically saying were *not* the invention. The problem with this argument is that it does not gibe with what the patentee actually said during prosecution. There, as noted above, the patentee explained that "[t]he claims detect attempted deception in an electronic communication by identifying communications where the sender *appears trustworthy in the communication but is not*. *Current approaches do not perform such a determination*." (D.I. 32, ex. A at 139 (emphasis added)) Put

But the inquiry here is not whether claim 14 is directed to something *new*. *See Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1151 (Fed. Cir. 2016) ("[A] claim for a *new* abstract idea is still an abstract idea.") (emphasis in original). The inquiry is whether the claim is directed to *an abstract idea*. And both in the patent and in the prosecution history, the patentee described the claims as being directed to "a mere result[,]" *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1305 (Fed. Cir. 2018): the general concept of "identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly."

In this way, and despite Plaintiff's argument to the contrary, (D.I. 34 at 13), the claim is unlike that at issue in *Finjan v. Blue Coat Sys., Inc.*, 879 F.3d 1299 (Fed. Cir. 2018). In *Finjan*, the Federal Circuit reviewed a district court's post-trial decision that the patent-in-suit was patent eligible. *Id.* at 1302. In doing so, the Federal Circuit concluded at *Alice*'s step one that the representative claim at issue was not directed to an abstract idea (e.g. "computer security writ large") but instead to a "non-abstract improvement in computer functionality[.]" *Id.* at 1305. The representative claim at issue was to a method of providing computer security by performing a particular type of behavior-based virus scan on a "downloadable" (an executable application program) and attaching the results of that scan to the downloadable itself in the form of a "'security profile.'" *Id*. at 1303. The *Finjan* Court noted that the claim passed *Alice*'s first step, in part because the evidence indicated that it "employs a new kind of file that enables a computer security system to do things it could not do before." *Id*. at 1305. But the Federal Circuit also

differently, the patentee explained to the Examiner that the prior art filters did not include the concept of "identifying deceptive messages that appear to be from a trustworthy source." Instead, those prior art solutions used blunter instruments (i.e., a blacklist, or a whitelist, which do not make any effort to determine whether a message appears trustworthy, and instead simply assesses whether certain words or e-mail addresses are on pre-existing lists) to try to weed out deceptive e-mails. (*Id.*; *see also* Plaintiff's Hearing Presentation, Slide 10)

explained that the claim survived step one not just because it had identified a "new" solution, but also because the claim was directed to "more than a mere result[.]" *Id.* Instead, the claim's central focus was on "specific steps—generating a security profile that identifies suspicious code and linking it to a downloadable—that accomplish the desired result." *Id.* Yet the claim at issue here is unlike that in *Finjan*. Use of claim 14's method does not result in the generation of a new type of computer file. (Tr. at 27; *see* Defendants' Hearing Presentation, Slide 24) And here, unlike in *Finjan*, when the patentee explained (in the specification and in the prosecution history) why the claimed solutions were new and better than the prior art, it never really focused on any "specific steps" used to accomplish the result sought. (D.I. 36 at 7) Instead, the patentee focused on the result itself—i.e., by articulating (broadly) that the claims simply allow for a way to identify messages that appear trustworthy, but in fact are actually deceptive, and to take action with regard to those messages.

For these four reasons, the Court agrees with Defendants that claim 14 is directed to the abstract idea of "identifying deceptive messages that appear to be from a trustworthy source and taking action accordingly." It thus proceeds to step two.

2. *Alice*'s Step Two

At step two, Defendants argue that nothing in claim 14 transforms the claim into a patent-eligible application. (D.I. 32 at 19-25) In response, Plaintiff focuses on the fact that the claimed method: (1) makes use of a content "database" that contains information about how the display name of an "authoritative entity" would be expected to be represented; and (2) then computes a "similarity distance" between the descriptor extracted from the incoming message and this information about the authoritative entity. (D.I. 34 at 20) And Plaintiff again notes that the

patentee, both in the patent and during prosecution, emphasized that prior art solutions did not make use of these analytic options. (*Id*. (citing D.I. 32, ex. A at 139; '628 patent, col. 3:15-26))[10]

If the step two question was solely about whether these limitations help demonstrate that there is a question of fact about whether claim 14's method was *new*, the result here would be an easy one, and favorable to Plaintiff. The patent says that it is. But this inquiry is also not about novelty. *Symantec*, 838 F.3d at 1318 ("[T]he [step two] inquiry is not whether conventional computers already apply [an abstract idea]."); (Defendants' Hearing Presentation, Slide 17). And if "the claim's only 'inventive concept' is the application of [the] abstract idea using conventional and well-understood techniques, the claim has not been transformed into a patent-eligible application of an abstract idea." *BSG Tech LLC v. Buyseasons, Inc*., 899 F.3d 1281, 1290-91 (Fed. Cir. 2018). Put differently, "a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention 'significantly more' than that ineligible concept." *Id.* at 1290.

Here, as noted above, the claim's computation of a "similarity distance" between a display name on an e-mail and an authoritative entity's display name can be achieved simply by

[10] There is no question that the inventive concept here cannot come from the claim's utilization of computer hardware and software to perform the method. The patent makes clear that the invention can make use of "standard commercially available server hardware" and "a typical server-class operating system[.]" ('628 patent, col. 6:37-42); *see also Bozeman Fin. LLC v. Fed. Reserve Bank of Atlanta*, 955 F.3d 971, 979 (Fed. Cir. 2020) ("[T]he use of well-known computer components to collect, analyze, and present data . . . does not render these claims any less abstract."). Moreover, the second claimed step of "determin[ing] . . . that the electronic communication was not transmitted with authorization from the authoritative entity" cannot amount to the inventive concept, ('628 patent, col. 36:4-6), as that portion of the claim does not provide any indication of *how* such a determination is made. *Cf. Two-Way Media Ltd. v. Comcast Cable Commc'ns*, 874 F.3d 1329, 1337 (Fed. Cir. 2017) ("The claim requires the functional results of 'converting,' 'routing,' 'controlling,' 'monitoring,' and 'accumulating records,' but does not sufficiently describe how to achieve these results in a non-abstract way."). Nor does Plaintiff argue that the third claimed step of "perform[ing] an action" on the message, ('628 patent, col. 36:19), amounts to an inventive concept, (Tr. at 70-71).

determining that there is a "match" between the two. And the existence of a "match" can be confirmed simply by "determining that the compared items are the same[.]" ('628 patent, col. 35:41-60) The Court agrees with Defendants that accomplishing this step simply "reflect[s] the abstract idea" itself. (D.I. 36 at 9, 11; *see also* Tr. at 38) That is, the act of determining that the name of a sender of an e-mail message and the name of the authoritative entity are or are not "the same" (something that a human or a computer could do) really seems no different from the general concept of "identifying deceptive messages that appear to be from a trustworthy source." *Cf. Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016) ("[W]e have treated analyzing information by [the] steps people go through in their minds . . . without more, as essentially mental processes within the abstract-idea category.").

As for the fact that the claim utilizes a computer "database" to store display name information for the authoritative entity—and then matches a piece of data against that information—this too cannot amount to an inventive concept. Instead, this step is simply an example of using computers in a way that is "purely conventional" and that exploits "one of the most basic functions of a computer." *Alice Corp.*, 573 U.S. at 225; *see Bozeman Fin. LLC v. Fed. Reserve Bank of Atlanta*, 955 F.3d 971, 979 (Fed. Cir. 2020) (concluding that claims were patent-ineligible where they "obtain information from financial databases and present results of a comparison of those pieces of financial information"); *see also Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1056 (Fed. Cir. 2017) ("The use and arrangement of conventional and generic computer components recited in the claims—such as a database, user terminal, and server—do not transform the claim, as a whole, into 'significantly more' than a claim to the abstract idea itself."). Therefore, the Court cannot see how these limitations, either

standing alone or considered in combination with the remainder of the claim, could provide the necessary "inventive concept."

3. Conclusion

For the foregoing reasons, the Court concludes that claim 14 is patent ineligible (and thus, all other asserted claims other than claims 4 and 5 are ineligible).

C. Claims 4 and 5

Lastly, the Court turns to claims 4 and 5. Those claims are in turn dependent on claim 2, which is dependent on claim 1. Claim 1, which is to a "classification system[,]" ('628 patent, cols. 33:55-34:58), but otherwise is essentially no different than claim 14, will not be reproduced here. Claims 2, 4 and 5 read:

> **2.** The system of claim **1** wherein determining that the electronic communication appears to have been transmitted on behalf of the authoritative entity includes evaluating text present in a body portion of the electronic communication.
>
> **4.** The system of claim **2** wherein evaluating the text includes evaluating the text using a collection of terms.
>
> **5.** The system of claim **2** wherein evaluating the text includes performing an equivalence analysis.

(*Id.*, cols. 34:59-62, 35:1-4)

Plaintiff contends that these claims provide "non-conventional ways of evaluating the text in the body portion of the email, by 'evaluating the text using a collection of terms' and 'performing and equivalence analysis.'" (D.I. 34 at 20; *see also* '628 patent, col. 35:1-4)[11]

[11] The patent describes how an embodiment of the invention might use a "collection of terms" to help determine if an e-mail is fraudulent, wherein the presence of a greater number of such terms (i.e., terms typically associated with fraudulent messages) in an e-mail could increase the likelihood that the e-mail is indicative of fraud. ('628 patent, col. 28:4-34 & FIGs. 23A-23B) Where multiple such terms appear on a given row in a collection of terms, the patent

However, the Court cannot see how claims 4 and 5 add an inventive concept. (Defendants' Hearing Presentation, Slides 35-36)

With respect to claim 4, the specification states that humans can create the "collection of terms." More specifically, under the title "Obtaining Collections of Terms," the specification states that, for example, "a human administrator . . . can manually create a given collection[.]" ('628 patent, col. 31:21-26) And no further detail is provided as to *how* the "collection of terms" is created or should be utilized as part of the invention. With respect to claim 5, the specification notes that, *inter alia*, an "equivalence class contain[s] common versions of the term. For example, the equivalence class for 'ACME Bank' contains 'A-C-M-E Bank,' 'AKME Bank,' and 'ACMAY Banc.'" (*Id.*, col. 11:31-34) Surely, if a human could generate a "collection of terms," it could also generate an "equivalence class." And as with claim 4, claim 5 does not provide any further information about *how* to perform an "equivalence analysis" or create an "equivalence class." Therefore, claims 4 and 5 do not include an inventive concept. *See Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1341-42 (Fed. Cir. 2017) (finding claims that "merely describe the functions of the abstract idea itself[] without particularity . . . [are] simply not enough under step two" and noting "the claim language . . . provides only a result-oriented solution, with insufficient detail for how a computer accomplishes it"); *Mortgage Grader, Inc. v. Costco Wholesale Corp.*, 89 F. Supp. 3d 1055, 1064 (C.D. Cal. 2015), *aff'd sub nom. Mortgage Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314 (Fed. Cir. 2016) (finding claims patent ineligible at step two where "nothing in the

---

describes those as an "equivalence class—terms that fulfill the same purpose if used in the story." (*Id.*, col. 28:6-8)

claim requires that the human 'be taken out of the loop'"). Therefore, the Court concludes that claims 4 and 5 of both patents are also patent ineligible.

IV. CONCLUSION

For all of the above reasons, the Court recommends that the District Court GRANT Defendants' Motions. Because Plaintiff has not suggested anywhere in its briefing that the issues at play could turn on claim construction, and in light of the nature of the Court's decision above (which does not suggest that further amendment of Plaintiff's pleading could change the outcome here), the Court recommends that the grant of the Motions be with prejudice. (D.I. 36 at 10-11)

This Report and Recommendation is filed pursuant to 28 U.S.C. § 636(b)(1)(B), Fed. R. Civ. P. 72(b)(1), and D. Del. LR 72.1. The parties may serve and file specific written objections within fourteen (14) days after being served with a copy of this Report and Recommendation. Fed. R. Civ. P. 72(b)(2). The failure of a party to object to legal conclusions may result in the loss of the right to *de novo* review in the district court. *See Sincavage v. Barnhart*, 171 F. App'x 924, 925 n.1 (3d Cir. 2006); *Henderson v. Carlson*, 812 F.2d 874, 878-79 (3d Cir. 1987).

The parties are directed to the Court's Standing Order for Objections Filed Under Fed. R. Civ. P. 72, dated October 9, 2013, a copy of which is available on the District Court's website, located at http://www.ded.uscourts.gov.

Dated: November 20, 2020

Christopher J. Burke
UNITED STATES MAGISTRATE JUDGE